

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently Amended) A processor implemented method of digitally managing the transfer of financial instruments between a ~~third party emitter~~, a first party owner and a second party transferee, the method comprising the steps:

a third party emitter issuing to the owner a title for a financial instrument, the title including (i) a message describing the title and how to contact the emitter, and (ii) a digital signature of the emitter;

the owner transferring ownership of the financial instrument to the second party transferee, including the steps of

the owner, ~~using a public signature scheme of the owner, signing the title by appending a message to the title, said message including adding~~ a public part of a signature scheme of said second party transferee to the title to produce an expanded title; and

the owner producing an owner message including the public part of the signature scheme of the transferee, and the owner signing the owner message using a secret key of a signature scheme of the owner.

2. (Previously Presented) A method according to Claim 1, wherein the transferring step includes the step of the emitter appending to the title a number indicating the number of successive owners of the title.

3. (Previously Presented) A method according to Claim 1, further comprising the step of the owner keeping the public part of the signature of the second party transferee and making said public part available to potential subsequent buyers.
4. (Previously Presented) A method according to Claim 1, further comprising the step of sending the title, with the signature of the owner made using the public signature scheme of the owner, to said second party transferee.
5. (Original) A method according to Claim 1, wherein the creating step includes the step of using a secure cryptographic generator to create the title.
6. (Original) A method according to Claim 5, wherein the secure cryptographic generator is an IBM 4758.
7. (Currently Amended) A system for digitally managing the transfer of financial instruments between ~~a third party emitter~~, a first party owner and a second party transferee, the system comprising one or more processor units configured for:
~~means for~~ a third party emitter to issue to the owner a title for a financial instrument, the title including (i) a message describing the title and how to contact the emitter, and (ii) a digital signature of the emitter; and

~~means for~~ the owner to transfer ownership of the financial instrument to the second party transferee, including ~~means for the owner to sign the title, using a public signature scheme of the owner, by appending a message to the title, said message including adding a~~

public part of a signature scheme of said second party transferee to the title to produce an expanded title; and

the owner producing an owner message including the public part of the signature scheme of the transferee, and the owner signing the owner message using a secret key of a signature scheme of the owner.

8. (Currently Amended) A system according to Claim 7, wherein the means to transfer ownership includes ~~means for the emitter to append~~ appending to the title a number indicating the number of successive owners of the title.

9. (Currently Amended) A system according to Claim 7, ~~further comprising means wherein the one or more processor units are further configured~~ for the owner to keep the public part of the signature of the second party transferee, and to make said public part available to potential subsequent buyers.

10. (Currently Amended) A system according to Claim 7, ~~further comprising means wherein the one or more processor units are further configured~~ for sending the title, with the signature of the owner made using the public signature scheme of the owner, to said second party transferee.

11. (Currently Amended) A system according to Claim 7, wherein the ~~means for creating includes one or more processor units include~~ a secure cryptographic generator for issuing the financial instrument.

12. (Cancelled).

13. (Currently Amended) A program storage device readable by ~~machine one or more processor units~~, tangibly embodying a program of instructions executable by the ~~machine one or more processor units~~ to perform method steps for digitally managing the transfer of financial instruments between a ~~third party emitter~~, a first party owner and a second party transferee, ~~said method steps comprising and wherein when executed, the program of instructions cause the one or more processor units to perform the steps of:~~

a third party emitter issuing to the owner a title for a financial instrument, the title including (i) a message describing the title and how to contact the emitter, and (ii) a digital signature of the emitter;

the owner transferring ownership of the financial instrument to the second party transferee, including the steps of

the owner, using a public signature scheme of the owner, signing the title by appending a message to the title, said message including a public part of a signature scheme of said other person second party transferee.

14. (Cancelled).

15. (Previously Presented) A program storage device according to Claim 13, wherein said method steps further comprise the steps of the owner keeping the public part of the signature of the second party transferee, and making said public part available to potential subsequent buyers.

16. (Previously Presented) A program storage device according to Claim 13, wherein said method steps further comprise the step of sending the title, with the signature of the owner made using the public signature scheme of the owner, to said second party transferee.

17. (Cancelled)

18. (Cancelled)

19. (Previously Presented) A method according to Claim 1, wherein:
said signature scheme includes a private key and a public key; and
the step of the owner signing the title includes the step of the owner using the public key of the signature scheme to encrypt the owner's signature in the title.

20. (Previously Presented) A method according to Claim 19, wherein the transferring step includes the steps of:

appending to the title a number indicating the number of successive owners of the title;
and
said second party transferee using said private key of the signature scheme to decrypt the owner's signature and said number.

21. (Currently Amended) A method according to Claim 1, wherein:
the digital signature of the emitter includes a public key of a public/private key pair of the emitter;

the issuing step includes the step of making a serial number and a description of the title publicly available as soon as the title is created;

the transferring step includes the steps of, after the public part of the signature scheme of said second party transferee is appended to the title,

- i) communicating to the emitter said public part of the signature scheme of said second party transferee,
 - ii) sending to the emitter a number N indicating the number of successive owners of the title,
 - iii) the emitter keeping said public part of the signature scheme of said second party transferee and making said public part of the signature scheme of said second party transferee available to potential future buyers, and
 - iv) ~~the emitter re-signing the title, and sending the re-signed title to said second party transferee, and~~
 - v) ~~the emitter posting that there is a new owner of the title and describing the public part of the signature scheme of said second party transferee; and~~
- a fourth party potential buyer asking the emitter to freeze the possibility of selling the title to anyone other than said fourth party for a period of time.

22. (Previously Presented) A method according to Claim 21, wherein:

the emitter is comprised of a set S of geographically distributed servers; and the issuing step includes the steps of

- i) using a signing key to make the digital signature of the emitter, said signing key including a plurality of partial keys,
- ii) sharing the signing key between the set of servers, wherein each of the servers has one of said partial keys,
- iii) at least some of the servers signing the title using a distributed protocol and using the partial keys of the servers,
- iv) considering the title signed by the emitter only if a defined subset of the S servers sign the title,
- v) using specified hardware to issue the title, and
- vi) using the specified hardware to print lists of title numbers and descriptions of the public part of the signature scheme used by the emitter.

23. (Currently Amended) A method according to Claim 1, wherein the transferring step includes the step of, after said message is appended to the title:

communicating to the emitter said public part of the signature scheme of said second party transferee;

the emitter keeping said public part of the signature scheme of said second party transferee and making said public part of the signature scheme of said second party transferee available to potential future buyers[[; and]]

~~the emitter re-signing the title, and sending the re-signed title to said second party transferee.~~

24. (Previously Presented) A method according to Claim 1, comprising the further step of a fourth party potential buyer using the emitter to prevent the sale of the title to anyone other than said fourth party for a defined period of time.

25. (New) The method according to Claim 1, wherein the method comprises the further step of the emitter signing the expanded title.